Network Security

CS 6823 - Lecture 1
Security Basics

Phillip Mak
pmak@nyu.edu

Lesson Objectives

- Define and explain basic security terminology
- Explain how vulnerabilities in one system affects another system
- Define the difference between Asset Owner and IT Asset Owner
- Perform Quantitative & Qualitative risk assessment
- Be able to perform analysis on attack trees

Network Security

- Most topics in Computer Science are focused on achieving a desired behavior

- Computer and Network Security is focused on preventing *undesired* behavior

  - Need to think differently
  - Paranoia is actually a good thing!
  - Enemy is going to try and find a input or state in your system which allows for a circumvention of protection measures.

Think Differently

- Security Mindset
  - What is the system designed to do? What is the proper operation?

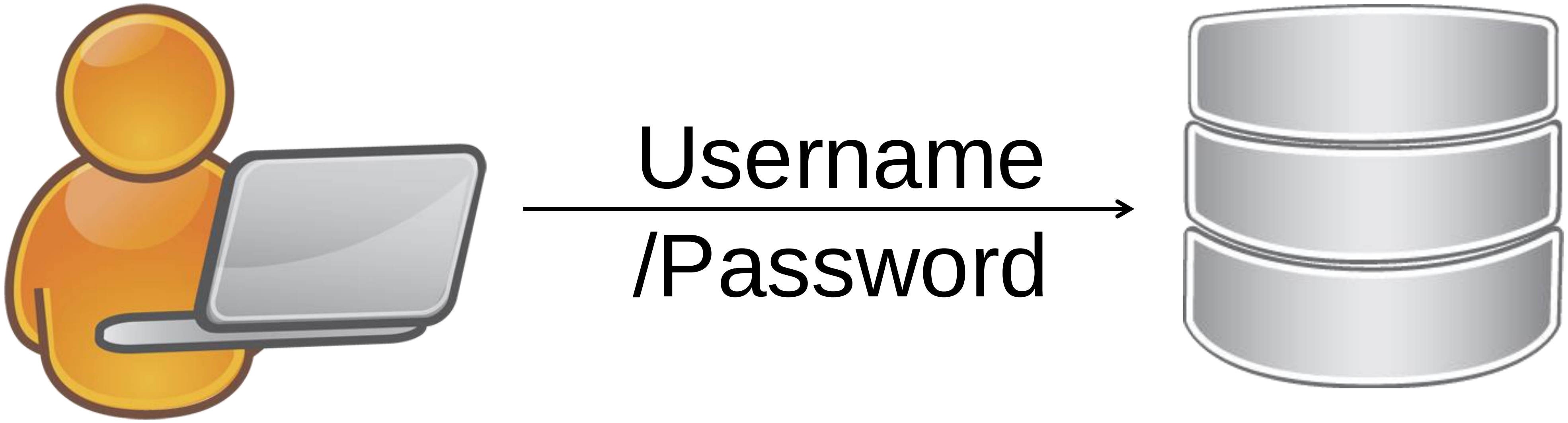
    The system is typically larger than just the computer or network. However for the purposes of this course we will focus on these parts. (Others, physical, human behavior)

  - What are the vulnerabilities in the system? How can this system be attacked?

  - How can the system be defended?

  - Is the cost of the defense worth it?   -Important concept!

Simplistic View on Password Authentication



Username

/Password

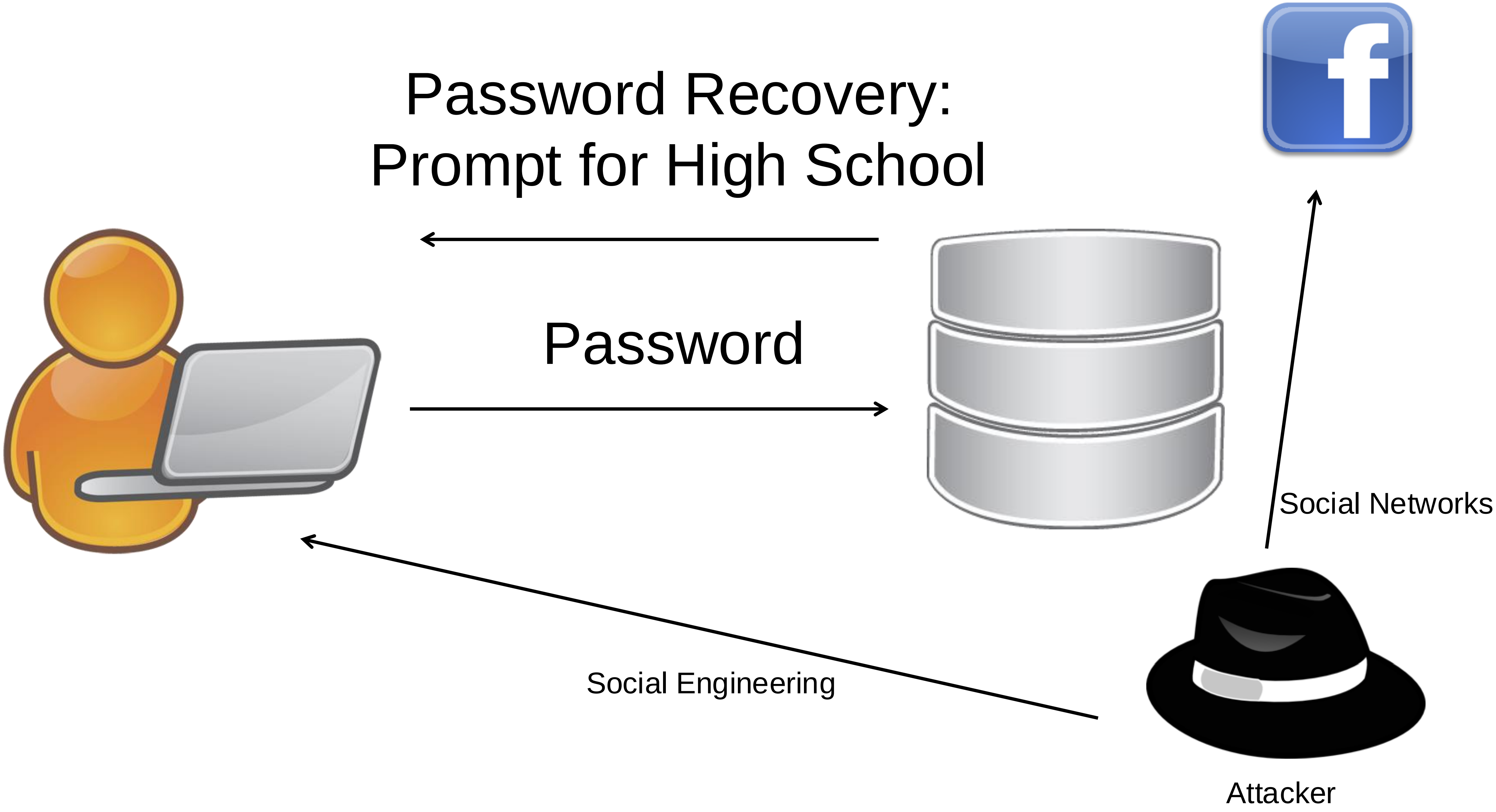
Exercises

- Each week, there are optional, bonus exercises during the lecture. All these exercises combined give a 2% added on top of your final grade

- Exercises are not checked for correctness, only for completeness.

- Submit exercises before the next class in the Assignment “Week #01 Bonus Exercise” in Gradescope

Reality – Larger System in Play



Attack on Wired Magazine Writer 2012 (1 of 3)

- Attacker’s goal was to take the targets twitter handle @mat
- Could directly attacker Twitter’s authentication but…
- Attacker found from the Twitter page the personal home page of the account holder
- There he found his gmail address
- Went to Google’s account recovery page
- The recovery page showed that he had an alternate email ending in @me.com
- Attacker new he could recover a @me.com email with just the billing address and last four digits of the associated credit card

Full details from the author

Attack on Wired Magazine Writer 2012 (2 of 3)

- Attacker could get credit card info from a “loophole” in Amazon
- Call Amazon and tell them you are the account holder and want to add a credit card. To do this the attacker just needs the email and billing address of the account holder.
- Got billing address since the victim registered a domain name for his website.
- Call back Amazon and indicate you lost access to your email account. Provide name, address and the new cc#
- Amazon sends account info to new email address held by attacker

Attack on Wired Magazine Writer 2012 (3 of 3)

- Attacker then could login and see last four digits of original cc#.

- Went back to Apple and took over @me and iCloud account (which are linked)

- Since @me was recovery email from Google and Twitter the attacker now took over those accounts as well.

- Wiped victims computer remotely using iCloud “feature”

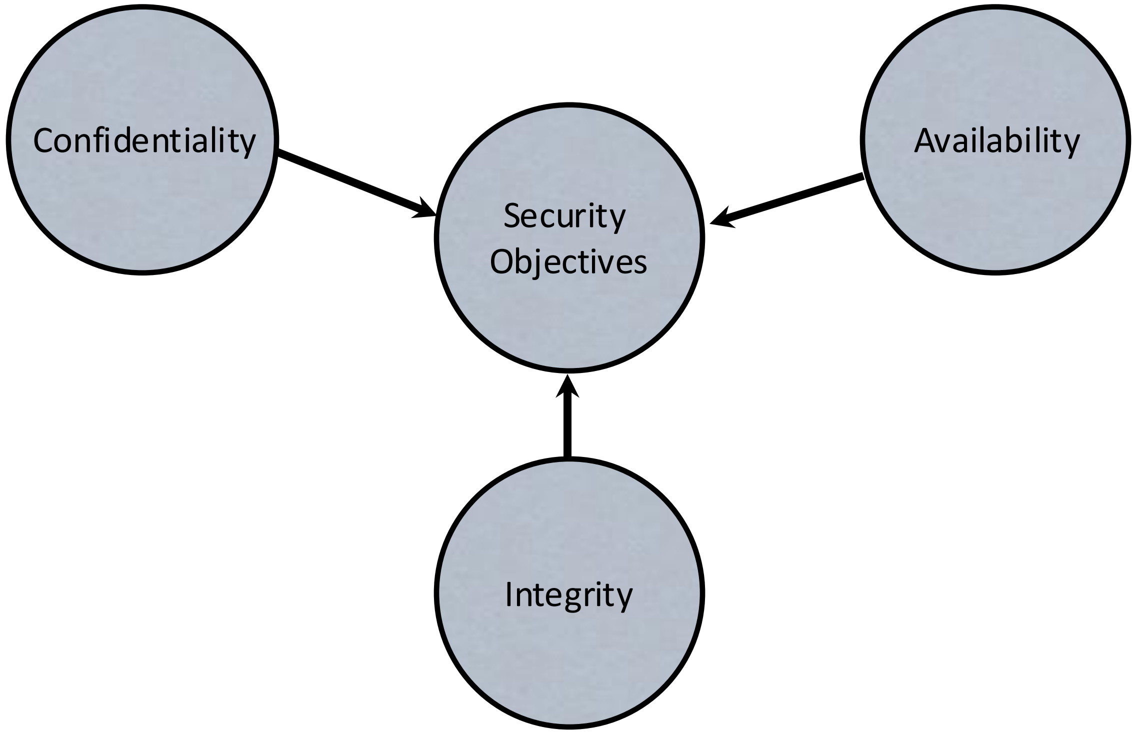
- What are the bounds of this security system?

The Cast of Characters

- The Cast of Characters
- Alice and Bob are the good guys
- Trudy is the bad guy (gal)
    - Stands for “Intruder”

CIA - You will see this in many textbooks

- **Confidentiality** - keeping information secret from unauthorized users
- **Integrity** - insuring that the information is genuine and hasn't been tampered with.
- **Availability** - ensuring that the system is always available.
- *Also add:*
  - ***Authenticity*** – determining the origin of data – Type of Integrity
  - ***Non-Repudiation*** – proving the integrity and origin – Type of Integrity



Good way to frame the problem.
But security is far more complex.

Alice’s Online Bank

- Alice opens Alice’s Online Bank (AOB)
- What are the security concerns for:
  - Alice (the bank)
  - Bob (the user)
  - Trudy (the attacker)
- Think about CIA-AN for each

CIA – on Alice's Online Bank (Example)

Confidentiality: prevent unauthorized reading of information

- AOB) must prevent Trudy from learning Bob's account balance
- Bob doesn't want the wrong people knowing his account details

Integrity: prevent unauthorized changing of information

- AOB must know what the account information is, and must prevent or detect tampering
- Bob must not be able to improperly change his own account balance
- Trudy must not be able to change Bob's account balance

Availability: Data is available in a timely manner when needed

- AOB's information must be available when needed
- Bob must be able to make transaction
- If not, he'll take his business elsewhere

Beyond CIA

- How does Bob’s computer know that “Bob” is really Bob and not Trudy?

- Bob’s password must be verified
  - This requires some clever **cryptography**

- What are security concerns of pwds?

- Are there alternatives to passwords?

When someone says “Their Network is Secure”

- What does this mean?

- Definition of Security – “Freedom from Risk or Danger”
  Random House Unabridged Dictionary

- Is it 100% protected against every conceivable threat?
  - No

- Is it impossible to attack and compromise
  - No

- Most of the time it means:
  - The network has been designed so as to maintain an acceptable level of risk.

Security is an engineering trade-off

- The objective is typically not to make the system secure against every threat.

- Instead the goal is to optimize the security of the system given certain constraints (cost, end user usability, information sensitivity)

Security is an ongoing process - not a product

- If a vendor comes to you and says that their “box” will secure your network - run!

- Security requires not only technical countermeasures and tools but processes and procedures.

- Once a tool, process or procedure is put in place it must be continuously revisited.

- **SECURITY IS PRIMARILY ABOUT RISK MANAGEMENT**

General Concept of Risk Analysis and Management

- A **risk** consists of something of value (an “asset” at risk) which may lose value if a negative event occurs.
- A **threat** to a system is any potential occurrence, malicious or otherwise, that can have an adverse effect on the assets and resources associated with the system.
- A **vulnerability** of a system is some characteristic that makes it possible for a threat to occur.
- An **attack (exploit)** on a system is some action that involves exploitation of some vulnerability in order to cause an existing threat to occur.

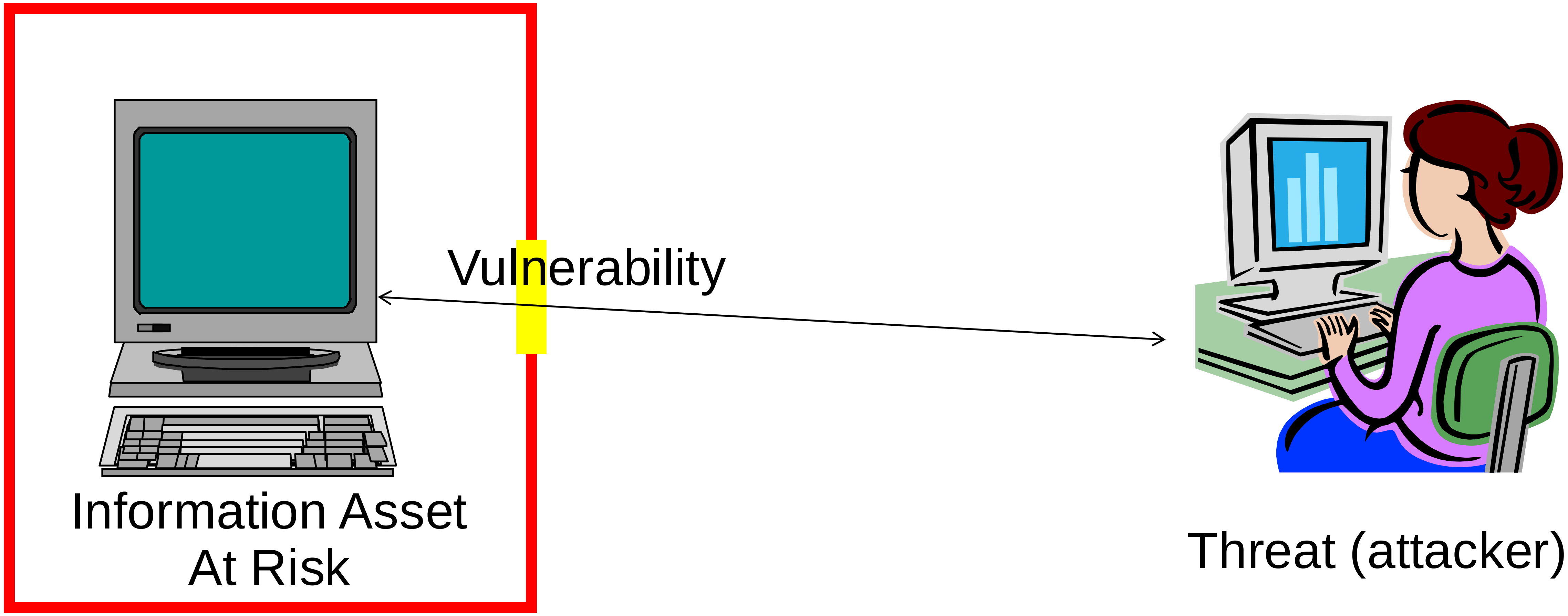
- Risk analysis is the process of:
  - Identifying the assets at risk
  - Putting quantitative or qualitative measures on the **likelihood** of the event happening
  - Putting quantitative or qualitative measures on the **consequences** of the potential loss (also called **impact**)

- Risk Management is a process for planning on how to **control** those risks

Non-IT Example 1: Driving risk

- Assets at risk: people's lives and health, the automobile, other property
- Negative event: auto accident
- Risk Management:
  - Risk **avoidance**: Don't drive or just not driving on snowy days
  - Risk **mitigation**: Seat belts, air bags, "crumple zones" in auto design, following DWI laws, defensive driving techniques, ABS, driving slow
  - Risk **transfer**: insurance
  - Risk **acceptance**: residual risk of injury, deductible on insurance

Information Security Risk Concept



Vulnerability

Information Asset At Risk

Threat (attacker)

Risk analysis starts with understanding what assets are potentially at risk, what the threats are. This forms the basis for finding the “sweet spot” of putting in enough security to protect the value of the assets.

Information Security Risk Analysis

Example: in a system that uses personal information such as name, SSN, etc., “Identity theft” is a risk. The related IT asset at risk is the confidentiality of that information. The impact of a compromise is the potential for identity theft.

Example: in a battlefield communications system, human lives are at risk if the system cannot be used to call in support. The related IT asset is the availability of the system, and the impact of a failure is potential for loss of life

The risk management strategies that we consider are for the IT assets, but the impact is based on the real assets

Asset Owner vs. IT Asset at Risk Owner

- The owner of the asset may not be the owner of the related IT asset at risk:
  - Example: an "identity" that may be stolen is an asset of that person, but the related IT asset (SSN, etc.) is under the control of many other entities.
  - Example: a civilian undercover agent (spy) transmits information to which only he has access back to a military organization. If that military organization's system is compromised, the agent's life may be at risk
- If the owner of the IT system does not suffer the impact of a compromise, what is the motivation to pay for the needed controls for proper risk management?
  - Example: Target was breached by hackers between Nov 27 – mid-Dec and personal information for 70-110 million people were stolen. The potential impact of each compromise was on the credit card holders (fraud, identity theft), Target, and the credit/debit card companies (which cover all fraudulent transactions above $50 per account by law).
- Laws and policies are required so owners of IT assets include it in their risk analysis and risk management

RISK ASSESSMENT

Risk Assessment

- Assessment: measures the impact of an event, and the probability of an event (threat agent exploiting a vulnerability)

- Quantitative (objective) and Qualitative (subjective) approaches both used.

  - Quantitative approach:
    - Compute expected monetary value (impact) of loss for all “events”
    - Compute the probability of each type of expected loss

  - Qualitative approach: use Low, Medium, High; ratings; other categorical scales

Risk Management

- Remove the risk (**risk avoidance**) - Remove the system component or feature associated with the risk if the feature is not worth the risk.
- **Mitigate** the risk - Reduce the risk with countermeasures.
- **Transfer** the risk – Transfer to somebody else via insurance, warnings etc.
- **Accept** the risk – Risk is low but costly to mitigate - worth accepting. Monitor.
- The understanding of risks leads to policies, specifications and requirements.
- Appropriate security mechanisms are then developed and implemented.

Quantitative - Security Cost Risk Assessment

Exposure Factor (EF) = Percentage of asset loss caused by identified threat

Single Loss Expectancy (SLE) = Asset Value X Exposure Factor

Annualized Rate of Occurrence (ARO) = Estimated frequency a threat will occur within a year

- **Annualized Loss Expectancy (ALE)** = SLE x ARO

Example:

- Fire Damage to a building:
  - Asset Value: value of the building - $750,000
  - Single Loss Expectancy (SLE: Asset Value x Exposure Factor) - $250,000 (damage caused by the fire)
  - Annualized Rate of Occurrence (ARO) - .05 (5% chance every year that there will be a fire)
  - Annualized Loss Expectancy (ALE: $250,000 x .05) = $12,500

- So does a fire alarm system which costs $5000 to install and maintain yearly worth it?

- YES - Fire Alarm Cost < ALE

Network Security Example:

- Credit Card database stolen from online retailer via SQL injection:
  - Asset Value: Here the asset value is a bit nebulous so it sometimes is better to focus on the SLE

  - Single Loss Expectancy (SLE): If the database is stolen and/or damaged how much is it going to cost the company in PCI fines, lost business, consulting fees for security, etc. $1M is not unreasonable for a medium sized retailer.

  - Annualized Rate of Occurrence (ARO) - Can get this information from network consulting organizations or your insurance company. 5%

  - Annualized Loss Expectancy (ALE)= $1M x 0.05 = $50,000

- So does a web firewall which costs $24K make sense? Most likely, YES

Quantitative: Useful or Not?

- Pros:
  - Objective, independent process
  - Credibility for audit, management (especially corporate management)
  - Solid basis for evaluating cost/benefit of countermeasures
  - Quantitative risk assessment is the basis for insurance, risk managed portfolios, etc.

- Cons:
  - In most cases, it is difficult to enumerate all types of events and get meaningful data on probability and impact
  - Very time consuming, costly to do right
  - Many unknowns may give a false sense of control
  - Not reliable for “rare” events or “unthinkable” impacts

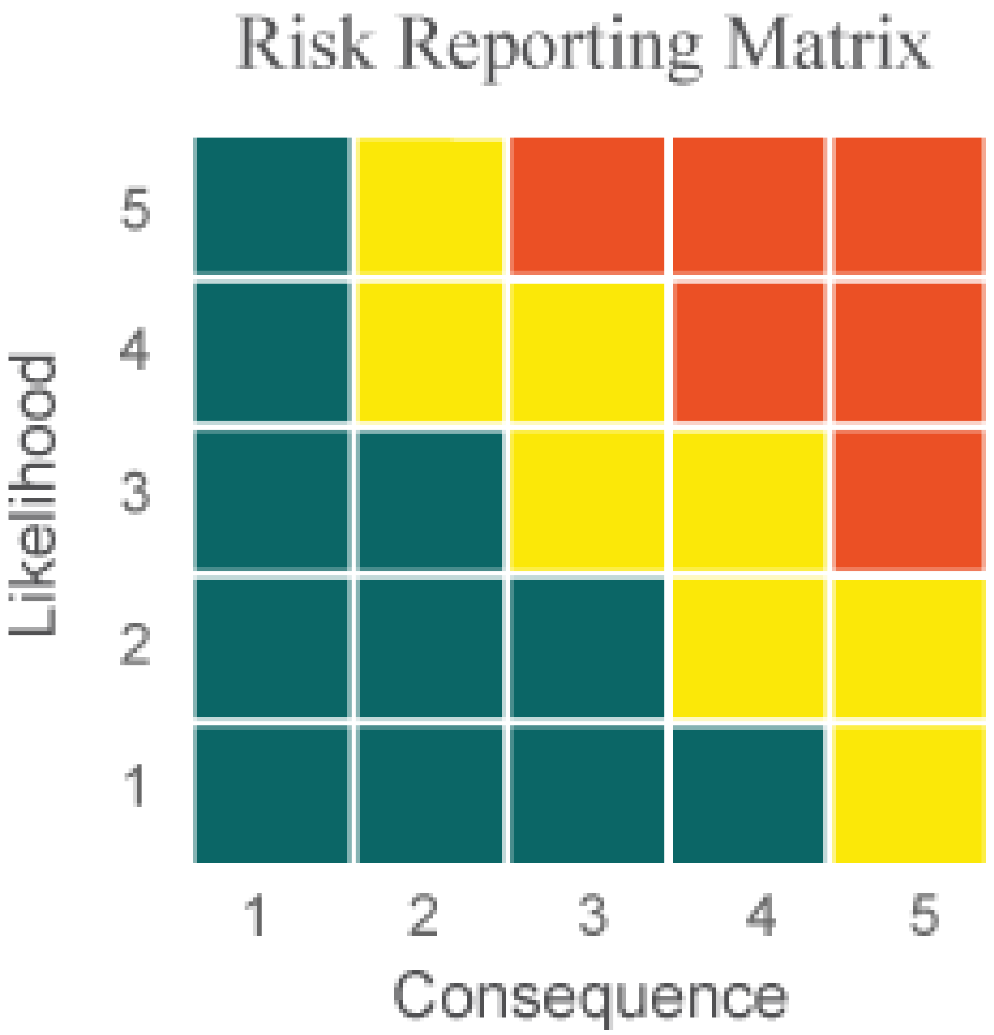
Qualitative Approach – Establish Impact

- Rather than have specific numbers, Establish classes of loss values (“impact”), such as:
  - Low, medium, high
  - Under $10K, between $10K and $1M, over $1M (used by at least one company)
  - Type of loss (e. g. compromise of credit card #, compromise of SSN, compromise of highly personal data)
  - Minor injury, significant injuries, loss of life, large scale loss of life (used by emergency response organizations to categorize non-IT events)
  - Rank ordering

Qualitative Approach – Establish Likelihood

- Establish classes of likelihood of compromise
  - Low, medium, high likelihood
- Decide on a risk management approach to each combination of (class of loss, likelihood of loss)
- Focus effort on medium to high loss and/or medium to high likelihood items

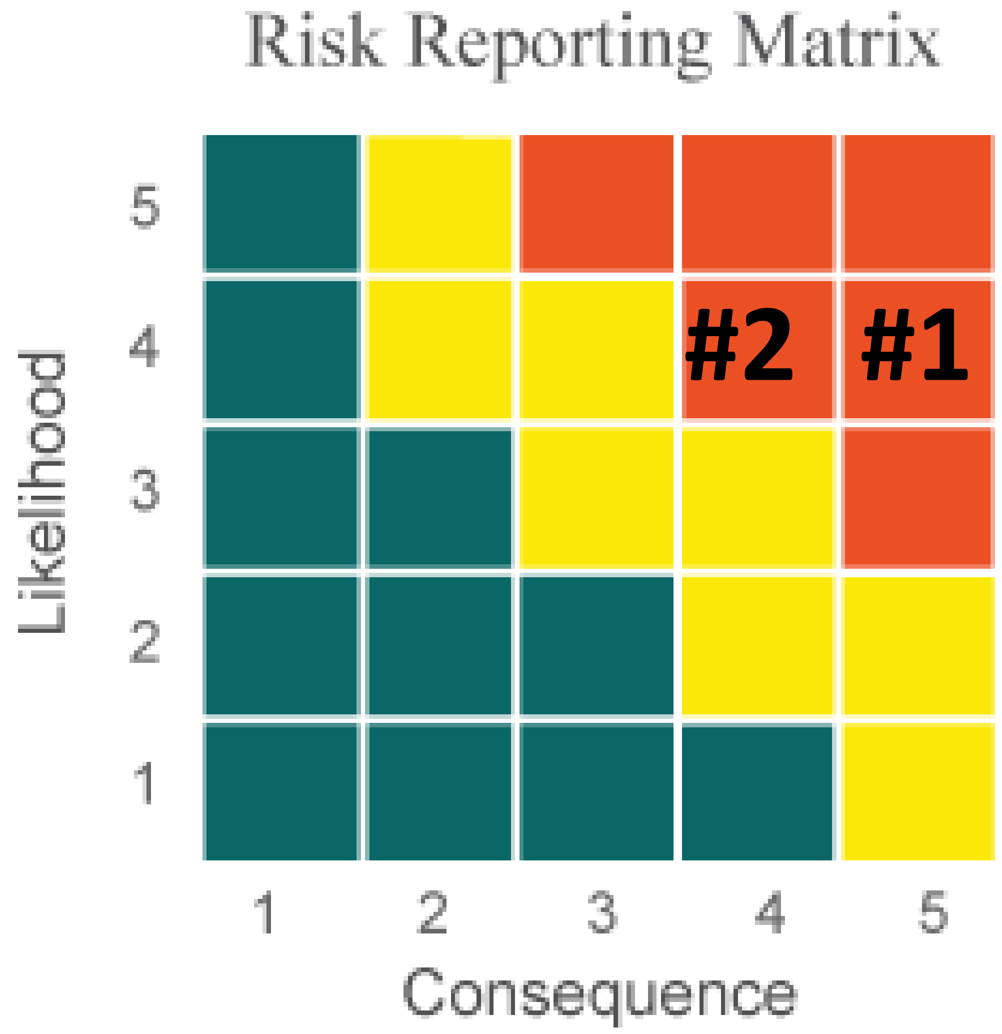
Risk Matrix



Level	Likelihood	Probability of Occurrence
5	Near Certainty	~ 90%
4	Highly Likely	~ 70%
3	Likely	~ 50%
2	Low Likelihood	~ 30%
1	Not Likely	~ 10%

Level	Consequences
5	Severe
4	Significant
3	Moderate
2	Minor
1	Minimal or no consequences

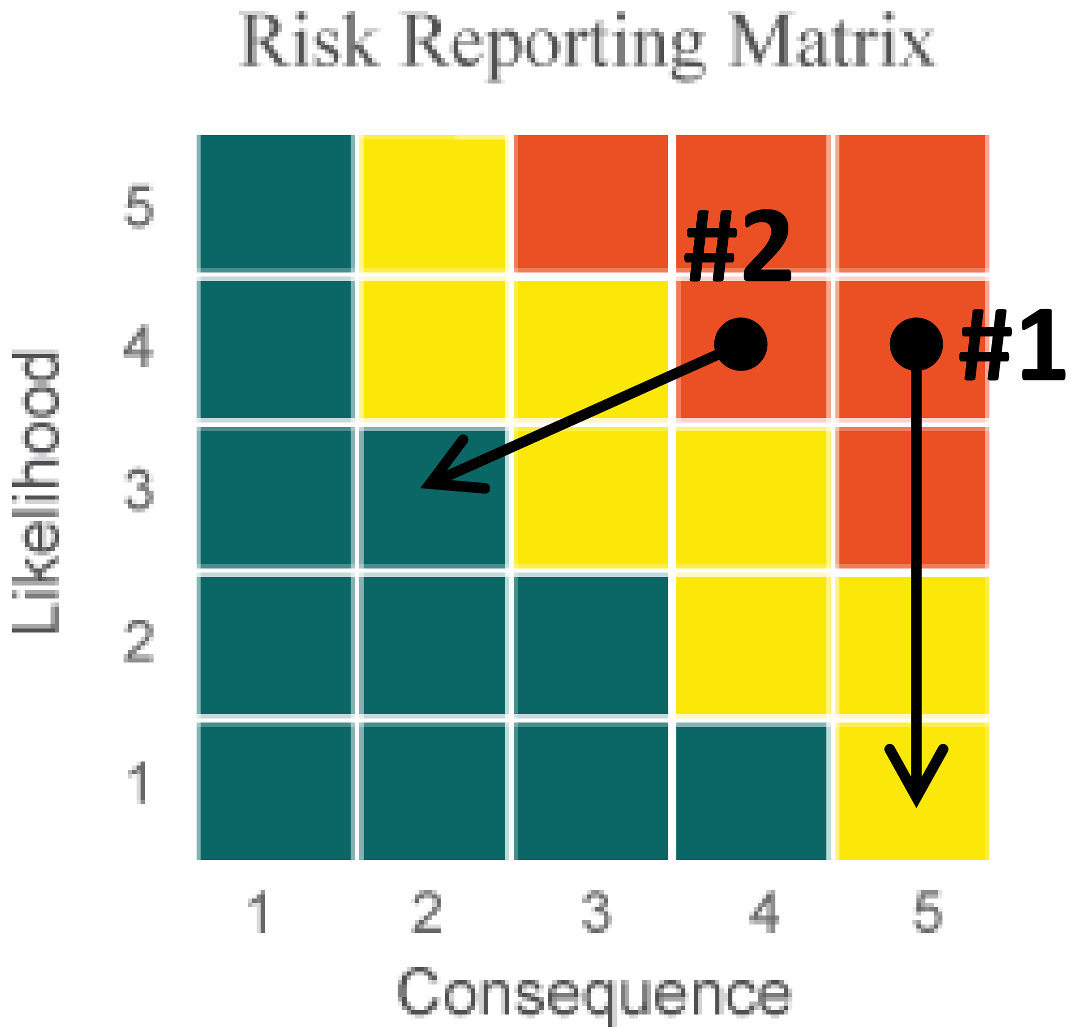
Example Risk Matrix (from the DoD)



Example Risk #1: The software is really buggy and will likely have buffer overflow vulnerabilities.

Example Risk #2: There’s a 70% chance the website will be hacked and one million credit card numbers will be lost.

Mitigating Risk



Example Risk #1: The software is really buggy and will likely have buffer overflow vulnerabilities. *Reduce the likelihood of this risk by spending more resources to reduce defects.*

Example Risk #2: There's a 70% chance the website will be hacked and 1 million credit card numbers will be lost. *Reduce consequences by not storing full credit card numbers. Likelihood reduced by adding a web firewall.*

Residual risk is the remaining risk after mitigations

Need to Stay Current!

- Do you have any good Security news sources? Please share in Slack #security-news